ORIGINAL

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	CC Docket No. 93-292
Policies and Rules Concerning	)	
Toll Fraud	)	

COMMENTS

MCI TELECOMMUNICATIONS CORPORATION

Mary J. Sisak
Donald J. Elardo
1801 Pennsylvania Avenue N.W.
Washington, D.C. 20006
(202) 887-2605

Its Attorneys

Dated: January 14, 1994

TABLE OF CONTENTS

SUMMARY

Service fraud is a serious problem that impacts consumers, telecommunications service providers -- both carriers and equipment suppliers -- and government. Fraud increases the costs of furnishing or receiving essential telecommunications services because they must be borne by someone. MCI therefore fully supports the development of policies, programs, and rules, if necessary, to incent affected parties to take the steps necessary to combat fraud effectively, and it is willing to become an active contributor in the efforts necessary to do so.

As recognized under current law -- and as evident from the application of pure common sense -- fraud accountability must reside in the person or entity controlling, or possessing the ability to control, the environment in which fraud occurs. Interexchange carriers, including MCI, cannot be responsible for fraud losses when fraud originates in the physical environment that lies beyond their service demarcation points. Thus, MCI cannot be held accountable for fraud losses involving its interexchange or international services when the fraud occurs via Customer Provided Equipment, including Private Branch Exchanges or cellular telephones, via local exchange or cellular carrier networks or network support systems, or via physical intrusions occurring at customer premises. In these circumstances, MCI is powerless to effect undertakings that could have prevented past fraud or might

foreclose fraud in the future. However, when fraud occurs as a result of some failure or compromise of MCI's network -- which MCI has responsibility for controlling -- then MCI is accountable for the resulting losses.

The Commission should exert a leadership role in bringing together affected parties to develop policies and programs to combat fraud, and it should sponsor legislation that improves the ability of law enforcement officials to investigate fraud and prosecute criminals who engage in fraud.

BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON, D.C. 20554

In the Matter of	)	
Policies and Rules	)	CC Docket No. 93-292
Concerning Toll Fraud	)	

COMMENTS

MCI Telecommunications Corporation (MCI) hereby provides its initial comments in response to the Commission's Notice of Proposed Rulemaking (NPRM) in the above-captioned proceeding.

I. INTRODUCTION

As recognized by the Commission, toll fraud is a significant problem affecting telecommunications users and providers alike. There are substantial steps that can and should be taken by affected parties -- customers, carriers, equipment manufacturers and vendors, and government -- to prevent or at least minimize the potential for toll fraud.

The Commission's goal should be to develop and implement policies that incent all affected parties to take those steps within their control to eliminate toll fraud. To accomplish this, the Commission should adopt an approach that holds accountable for fraud the person or entity that controls, or has the ability to control, the equipment and/or facilities through which fraud originates.[1] Thus,

---

[1] The Commission adopted this principle in the Chartways decision in which the Commission found that the PBX owner had control over the PBX and, therefore, was held liable for all

for example, if fraud were to result from of a failure or compromise of MCI's network, MCI should, (and does) accept responsibility for the problem. However, no entity should be held accountable for fraud or fraud losses when that entity does not-- or cannot-- control the environment that makes fraud possible.

As recognized by the Commission, customer education is important in combatting fraud. However, as discussed below, the Commission's proposals concerning carrier monitoring and liability apportionment-- once fraud has occurred-- will not be effective in preventing it. In addition, it is wrong to suggest that it is possible today to establish all measures customers can take to prevent fraud because methods to commit fraud are constantly evolving, and the technology available to detect and prevent fraud is constantly improving. Therefore, customers and carriers each have a continuing obligation to "keep current" in the fight against fraud.

Moreover, customers should not be insulated from responsibility for fraud, which apparently is intended by the Commission in connection with payphone and PBX owners. Insulating PBX and payphone owners from the financial consequences of fraud is contrary to the public interest because it would shift fraud costs to other carrier

---

calls originating at the PBX, including fraudulent calls. Chartways Technologies, Inc. v. AT&T, 6 FCC Rcd. 2942; affd on review 9 FCC Rcd. 5601 (1993).

ratepayers. Payphone owners are in the business of providing payphones to the public and, as a result, access to the public switched network. And PBX owners, typically, own or lease their own switches in order to possess greater control over their communications. Greater responsibility follows from greater control. Moreover, such insulation would serve to eliminate needed incentives to take steps necessary to minimize or prevent fraud.

MCI addresses the Commission's specific questions and proposals below.

II. FRAUD AWARENESS AND EDUCATION

Customer awareness and education concerning fraud is extremely important because, in most cases, customers are in the best position to prevent fraud. Accordingly, MCI voluntarily developed an extensive program to educate customers, equipment manufacturers and law enforcement officials about toll fraud. Thus, MCI provides informational brochures concerning toll fraud free-of-charge to anyone who requests them.[2] MCI also has established an 800 "helpline" to answer questions about toll fraud. In addition, MCI has sponsored and participated in hundreds of CPE toll fraud prevention seminars around the country, also free-of-charge.

---

[2] Copies of some of these brochures are appended hereto as Attachment A.

MCI also has produced two videos concerning toll fraud entitled "Phone Fraud - The Solution" and "Invisible Criminals," which are provided free-of-charge to businesses, government agencies, equipment manufacturers and vendors, telecommunications consultants and carriers.[3] MCI has even authorized carriers and equipment manufacturers, including AT&T, US West, Sprint, Pacific Bell, Bell Atlantic, British Telecom, Rolm and Northern Telecom, to show the video in conjunction with their fraud presentations.

However, the duty to inform customers about fraud cannot be placed solely on interexchange carriers (IXCs) because they do not have access to all customers. For example, local exchange carriers (LECs) are in a position to alert customers about fraud through bill inserts in monthly bills sent to customers.

In addition, IXCs may not know about all of the capabilities or changes made to customer equipment interconnected to IXC services. Therefore, equipment manufacturers and vendors also have obligations to inform customers concerning their equipment and fraud potential.

III. CPE FRAUD

Customer premises equipment (CPE) fraud, including private branch exchange (PBX) fraud, occurs when

---

[3] A list of some of the entities that have received and used the MCI videos is attached as Attachment B.

unauthorized persons gain access to a customer's communications services by compromising the customer's equipment. There can be no dispute that the customer controls -- or is capable of controlling -- its CPE.[4] Therefore, the customer should be held responsible for any fraud which occurs through its CPE.

MCI believes there is an obligation on the part of equipment manufacturers and vendors to provide sufficient information addressing the proper use and maintenance of CPE, including information concerning the potential abuses of the equipment and related services, in order to enable customers to make informed decisions concerning which CPE features to deploy. The Commission's suggestion, however, that common carriers may have some liability in connection with CPE fraud clearly misses the mark.

In the NPRM, the Commission tentatively concludes that carrier tariff liability provisions that fail to recognize an obligation by the carrier to warn PBX customers about the risks of using carrier services are unreasonable. The Commission also tentatively concludes that carriers have an affirmative duty to ensure that warnings are communicated to customers through billing inserts, annual notices or other methods.

As an initial matter, MCI's tariff warns <u>all</u> customers

---

[4] In any event, there is no way it could be found that an IXC is in a control position with regard to the equipment.

that they are responsible for all charges, even those that result from the misuse or abuse of their service by third parties. This has been in MCI's tariffs for many years. In addition, as noted above, MCI provides extensive information to customers concerning CPE fraud and the steps that can be taken to prevent it. It does so, not out of any sense of legal obligation, but, rather, because its interests are served by customers taking steps to prevent fraud from occurring.

The Commission is incorrect to suggest that MCI has a legal obligation to provide this information when MCI does not own, provide, control or maintain the CPE through which fraud occurs. Moreover, CPE fraud occurs because the equipment has been compromised -- not the interconnected carrier services. Thus, customers should be warned about CPE fraud risks but that warning should emanate from equipment manufacturers and vendors.

The Commission also seeks comment on whether the costs resulting from CPE-based fraud should be apportioned based on whether carriers, CPE owners, equipment manufacturers or others were in superior positions to avoid, detect, warn of, or control fraud. The CPE owner or lessee -- the person or entity with the capability to control the CPE on a day-to-day basis -- is in the best position to take steps to prevent fraud and, therefore, should be responsible for any fraud that occurs via the equipment. In addition, the CPE

owner or lessee is the only person with knowledge of whether calls are authorized. In this regard, there are capabilities that are standard in PBX equipment, such as station message detail reporting, that are extremely effective in helping to detect fraud. In addition, there are a number of software packages available on the market today which can be used by owners to analyze call records for fraud detection. Also, a number of equipment manufacturers make and furnish equipment that can be connected to CPE, to measure traffic against calling pattern thresholds and parameters pre-set by customers. This equipment notifies the CPE owner when the thresholds and parameters are exceeded.

Of course, equipment manufacturers and vendors should notify and fully inform their CPE customers about equipment capabilities. This suggests that they should be held accountable for any information they furnish that is incorrect or incomplete when fraud results from that information. Moreover, "fraud-prone" features should not be installed without the customer's informed consent.

Interexchange carriers clearly are not in a superior position to detect or control CPE fraud. An IXC most likely does not know the CPE features that the customer has activated and, even when it does, it has neither the authority nor the ability to reconfigure, or to compel the customer to reconfigure, the equipment to prevent fraud. In

addition, although IXCs can monitor traffic, they only "see" the traffic carried over their networks and, therefore, they lack a total picture of the customer's traffic or traffic patterns.[5] Furthermore, because IXCs must set general fraud thresholds in their monitoring equipment, the thresholds will not be exact for any one customer. And, even if an IXC detects a pattern of calling which appears to indicate the presence of unauthorized calls, the IXC cannot know for certain the status of those calls without actual contact and confirmation by the customer. Moreover, fraud frequently occurs after business hours and on weekends-- times when the customer cannot be reached to verify the calls. And, even when the customer confirms that calling is fraudulent, a carrier can only "block" calls to its network.[6] Thus, fraudulent calls still could be placed through the same customer facilities to other IXCs.

Finally, the Commission asks whether a carrier's failure to offer services to limit customers exposure to fraud should be considered unreasonable, and whether IXCs and LECs should be required to offer protection through monitoring services. The Commission also asks whether the fraud programs offered by MCI, AT&T and Sprint are

---

[5] This is particularly the case when an IXC provides only a segment or piece of the customer's telecommunications service, as frequently is the case.

[6] In addition, if the carrier "blocks" the calls, all calls will be blocked including proper ones placed during the period of blocking.

sufficient.

As demonstrated above, hardware and software to monitor traffic and assist in fraud detection are generally available in the marketplace at reasonable prices. Moreover, customers have the ability to institute CPE modifications in order to prevent or minimize fraud. Accordingly, there are available fraud prevention and detection options for acquisition and use in connection with the equipment through which fraud originates and, therefore, it is not necessary to require carriers to provide additional services. MCI, AT&T and Sprint do in fact provide fraud detection services which customers can use to augment their own monitoring efforts. Customers can choose from among these competitive offerings for the one best suited for them. Under the circumstances, the Commission should not mandate the furnishing of certain fraud programs because that would only serve to limit the competitive choices of consumers.

IV. PAYPHONE FRAUD

The Commission tentatively concludes that payphone owners (PPOs) who take "reasonable steps" to limit their exposure to toll fraud, such as purchasing originating line screening (OLS) and billed number screening (BNS) service, and are not "customers" of a carrier should not be held accountable for fraudulent calls made through their

equipment. The Commission then asks whether carriers should be required to modify tariff language limiting their liability for payphone fraud and whether there are any steps PPOs can take to prevent fraud.

The Commission already has found that there are steps PPOs can -- and should -- take, (in addition to purchasing OLS and BNS service) to protect themselves against fraud. For example, the Commission has determined that aggregators, including payphone providers, should be able to prevent fraudulent domestic direct-dialed calls through a reprogramming of payphones or through the addition of adjunct devices, and the Commission has required LECs to offer, where feasible, international blocking to aggregators to assist in preventing fraudulent international direct-dialed calling.[7] In addition, "cuckoo tones" could be installed in premises equipment by PPOs or in central offices of LECs to prevent fraudulent international collect calls, or LECs could assign blocks of numbers to payphones which would allow PTT operators to identify them.

The Commission's suggestion that not presubscribing to an IXC is somehow relevant to fraud prevention is incorrect because LECs still transmit 10XXX +1 calls from such payphones to IXCs. Therefore, fraudulent 10XXX +1 calls can

---

[7] In the Matter of Policies and Rules Concerning Operator Service Access and Pay Telephone Compensation, Order on Reconsideration, CC Docket No. 91-35, FCC 92-275, released July 10, 1992.

still be originated from payphones that do not "PIC" a primary interexchange carrier.

There also are other factors, such as those pertaining to the location and inspection of phones, and the type of phone equipment installed, that affect the incidence of fraudulent calling made from payphones. These factors are entirely within the control of the PPO and, therefore, PPOs must be held accountable for resulting fraud.[8] LECs and IXCs should not be made "insurers" of PPOs, thus rendering the latter risk-free and capable of engaging in inadequate business practices with impunity.

In addition, PPOs purchase OLS and BNS from LECs, not IXCs. PPOs, therefore, must seek redress from LECs for any fraud that results from any failure of those services. Moreover, even if a PPO purchases BNS from a LEC, there is no guarantee that fraudulent calls will not be billed to the phone because BNS service is only effective in preventing fraud when the data in the line information database (LIDB) is accurate and timely. Significantly, there is evidence before the Commission in the LIDB access tariff investigation that calls into question the integrity of the LIDB data. Accordingly, only LIDB providers are responsible for the integrity of LIDB data and, by extension, BNS service that is dependent upon LIDB information in

---

[8] In any event, there is no way it could be found that an IXC is in a control position with regard to payphones.

preventing fraud.

V. CELLULAR FRAUD

The Commission seeks comments on what the cellular industry, manufacturers, vendors, law enforcement agencies and the Commission can do to combat cellular fraud. The Commission also asks whether adequate incentives are in place to encourage the industry to develop anti-fraud solutions; whether a shared liability theory for cellular fraud is appropriate; and whether unique criminal legislation is necessary.

Cellular fraud primarily results from deficiencies in cellular network and equipment standards. For example, the majority of cellular fraud occurs when unauthorized persons "steal" the mobile identification number (MIN) and electronic serial number (ESN) of a subscriber's cellular phone and use them in another cellular phone to complete calls. It is an easy matter to "intercept" the MIN and ESN with widely available scanning equipment because they are transmitted during a valid call.[9] Once these numbers are obtained, they can be used in another cellular phone to complete calls because the cellular switch recognizes the numbers as valid.

---

[9] There are ways, however, to protect the transmission, such as through the use of encryption.

Clearly, IXCs should not be held liable for fraudulent cellular calls because the fraud occurs in the cellular network, and IXCs have no ability to determine whether a cellular call passed through to them is fraudulent. In addition, most cellular carriers do not send the information digits to the IXCs which are necessary to identify the call as cellular and, therefore, IXC monitoring would not be effective in detecting potentially fraudulent cellular calls.

VI. LIDB

The Commission states that LIDB customers, namely IXCs and operator service providers, have an obligation to query LIDB when accepting a LEC card for billing to determine whether the card is valid. The Commission asks whether the carriers querying LIDB should provide the LECs with the originating calling party number and the called number in order for the LECs to develop customer calling pattern profiles and set fraud parameters. The Commission further asks how the presence or absence of this information should affect any decision concerning the allocation of liability for toll losses and whether carriers should be permitted to charge for the provision of this information.

MCI queries LIDB when accepting a LEC card for billing. Unfortunately, because inaccurate data resides in LIDB, a card sometimes is approved as valid when it is not. In any

event, MCI must pay the LIDB query charge and access charges to the LEC, in addition to other costs that may be associated with the call, such as settlement payments to the foreign telephone company. Clearly, LECs have no incentive under this scenario to ensure the accuracy of LIDB as it receives the same payments for the valid and fraudulent calls.

In order to provide a proper incentive, LECs should be made financially responsible for the IXC tariffed charges for fraudulent calls that are "approved" by LIDB. At a minimum, LECs should not be permitted to collect the LIDB query and access charges associated with fraudulent calls.

Finally, with regard to the question of whether IXC's should be required to provide the originating and terminating number to LECs in order for the latter to set fraud parameters in their networks, MCI submits that IXCs should be required to provide this information only if the LECs are willing to assume full financial responsibility for any fraudulent calls they authorize.

VII. CLIP-ON FRAUD

Although the Commission does not address it in the NPRM, clip-on fraud is a growing problem that potentially affects all customers. Clip-on fraud occurs when unauthorized persons physically attach equipment to the telephone line -- either on the LEC's side of the

demarcation point or on the customer's side -- to make fraudulent calls. Because this type of fraud occurs at the line, LECs should be required to investigate clip-on fraud and take prompt corrective action when it is located. In addition, LECs should be financially accountable for clip-on fraud which occurs on the LECs' side of the demarcation point because it involves LEC facilities over which the LECs are in a superior position to control.[10]

VIII. ADDITIONAL COMMISSION ACTIONS

In addition to the proposals set forth above, the Commission could facilitate the reduction of certain types of fraud by facilitating the exchange of information necessary for the detection and investigation of toll fraud among service providers.

MCI investigators have often been stymied in their efforts to investigate instances of toll fraud because of the reluctance of certain LECs to provide needed assistance. For example, MCI investigators are often in possession of Automated Number Identification (ANI) information which they have reason to believe is directly involved in the fraudulent use of service, and require the associated customer name and address in order to further the investigation. However, even when informed that the

---

[10] In any event, there is no way it could be found that an IXC is in a control position with regard to facilities or equipment on the LEC side of the demarcation point.

requested information is directly related to a fraud investigation, some LECs have refused to provide customer name and address information for non-published customers, citing a need to preserve the customer's privacy. Providers of paging services also routinely refuse to disclose customer name and address information, even when the relevance of the requested information to a toll fraud investigation is demonstrated. In addition, IXCs need LEC customer account information in order to prevent subscription fraud and "carrier hopping;" that is, where a customer intends never to pay for its service and simply subscribes to a succession of carriers when its service is terminated for non-payment.

Accordingly, MCI urges the Commission to adopt policies and programs and, if necessary, rules requiring the exchange of customer information, as follows:

1. Customer name and address (including the names and addresses associated with non-published telephone numbers, paging devices or other telecommunications devices) should be disclosed in a timely fashion when requested, when such disclosure is necessary either to investigate fraud or prevent its occurrence.

2. Carriers should expeditiously disclose upon request all information in their possession that is relevant to a toll fraud investigation. The Commission should sponsor programs to facilitate the development and dissemination of

information related to toll fraud, such as a national subscription fraud data base, which would be available to fraud investigators.[11]

Finally, the Commission should investigate the practices of LECs with respect to their fraud detection activities. Specifically, LECs provide Dialed Number Recorders (DNRs) to monitor digits dialed from telephones identified as being used for criminal activity. DNRs record the dialed digits, regardless of which IXC carriers the interstate portion of the call. LEC charges to IXCs for the use of DNRs are excessive. In addition, it is not uncommon for a LEC to charge multiple IXCs and law enforcement agencies for the same information. Fraud deterrence, however, should not be a LEC profit center.

Accordingly, MCI urges the Commission to:

1. Require carriers to render assistance in the investigation of toll fraud and limit the charges, if any, for such assistance to reasonable charges incurred in providing the service.

2. Undertake as may be appropriate a study to determine fair compensation for the installation and operation of DNRs and consider whether such rates, if any, should be filed in LEC tariffs as are incident of their

---

[11] Information acquired should be held in confidence and not used for any other purpose than fraud detection, investigation or prevention.

furnishing services.[12]

3. Require carriers which become aware of telecommunications fraud affecting other carriers and/or their customers report promptly the information to the affected carriers or customers.

IX. LAW ENFORCEMENT EFFORTS

Finally, MCI urges the Commission to propose legislation to Congress that would give law enforcement officials a better ability to track and prosecute fraud. Telecommunications toll fraud requires a "federal solution" because, in most instances, the victim and the perpetrator are located in different states at the time the crime is committed and the calling conducted is interstate or international in nature. Currently, there are no federal criminal statutes that specifically prohibit the theft of telecommunications services. The most widely used statutes to prosecute telecommunications toll fraud are "Fraud and Related Activity in Connection with Access Devices", 18 USC 1029, and "Fraud by Wire, Radio or Television", 18 USC 1343. These statutes are not adequate, however, simply because they were designed for other purposes. For example, Congress enacted the access device statute to combat credit

---

[12] LECs should also be prohibited from assessing additional charges for ancillary services, such as "DNR Analysis," unless specifically requested, and in no event should such charges be "bundled" with any rate, if any, for DNR.

card fraud. Although calling cards and some codes used in the completion of telephone calls fall within the ambit of the statute, telecommunications fraud never was specifically addressed in the legislation and, accordingly, jurisdictional issues arise in prosecutions.[13] Similarly, the wire fraud statute was intended to address fraud occurring through the use of the telephone. The statute was not necessarily intended to address the unlawful avoidance of the payment of charges for use of the telephone network itself.

Therefore, because the criminal statutory landscape is lacking, MCI urges the Commission to support enactment of a federal criminal statute to combat telecommunications toll fraud. The statute, at a minimum, should:

1. Proscribe the unauthorized possession or illegal use of any device to evade or avoid the lawful payment of charges for telecommunications services. This would encompass the possession or use of so-called "blue boxes", "black boxes", calling card numbers, PBX and voice mail remote access feature authorization codes, and other similar

---

[13] For example, in Bailey v. United States, a United States District Court in California ruled that this statute did not apply to the defendant, even though a jury found that he was in possession of several cellular phones which had been altered to mask the identity of the owner and permit virtually unlimited unbillable calls.

devices, either existing or prospective.[14]

2. Proscribe the theft of telecommunications services or any scheme to facilitate the theft of telecommunications services.

3. Dedicate funding to address toll fraud in the budgets of the federal law enforcement agencies with investigative jurisdiction. The authority of the Commission to investigate toll fraud crimes could be expanded in a manner similar to the authority of the Securities and Exchange Commission to investigate securities irregularities.

In addition, serious consideration should be given to amending certain federal laws, which may hinder fraud investigations. For example, Section 2703 of Title 18 of the United States Code may impede the ability of carriers to report criminal activity to law enforcement agencies -- even when the crime involves the illegal use of a carrier's network -- by virtue of the requirement that a subpoena precede the disclosure of information. Accordingly, Section 2703 could be amended to make it clear that providers of telecommunications services may voluntarily disclose to law enforcement officials toll records and other information necessary to investigate fraud.

---

[14] It is important that legislation recognize the rapid, evolving nature of technology. Thus, the legislation should be sufficiently flexible in scope to reach avenues of fraud not yet even dreamed of or devised by criminals.

In addition, Section 2703 could be interpreted as precluding law enforcement agents from obtaining certain information from carriers, such as the customer's name, address, account number and primary interexchange carrier (PIC), in the absence of a subpoena. That provision could be amended or clarified to permit carriers to disclose customer name, address, account number and PIC information to governmental agencies in response to a formal written request by the agency.

In addition, Section 2511 of Title 18, which allows carriers to intercept fraudulent "wire communications," could be amended to allow for the interception of fraudulent "electronic communications." A "wire communication" is specifically limited to "aural transfers;" that is, "a transfer containing the human voice at any point between and including the point of origin and the point of reception." An "electronic communication", however, such as the interaction between a remote user and a computer, does not regularly involve the "transfer of the human voice". Carriers should be able to monitor electronic communications to insure the integrity of information stored on computer systems, particularly those with dial up access, and to keep out "hackers" and other unauthorized persons. Accordingly, Section 2511 could be amended to authorize system operators to intercept, disclose, or use electronic communications in order to combat or prevent fraud.